

REMARKS

The application has been amended and is believed to be in condition for allowance.

Claim 1 is the only independent claim.

Claim 9 has been amended to clarify that claim 9 depends from claim 1.

Claims 1-5, 7, and 9-12 were rejected as obvious over RATAYCZAK 6,259,909 in view of HODGES 5,420,908.

Claims 6 and 8 were rejected as obvious over RATAYCZAK in view of HODGES and further in view of FIELDER 5,995,624.

Applicants respectfully disagree; claim 1 having been amended to address the criticisms raised by the Official Action.

Claim 1 now specifies that the user is a person. The claim language provides an explicit distinction to distinguish the user from the user device.

This amendment is supported by the application specification. In the specification, the terms "user" and "client" are used as equivalent terms (see for example page 6, lines 8-9 and page 7, lines 1-2), a client being, according to the Application, "A person who request access" (page 1, lines 6-8). In particular, in reference to Figures 1-7 illustrating two examples of implementation of the invention, the disclosure language uses the term "client" (pages 11-16).

Page 20, lines 15-20 of the specification does not disclose a client device that generates an authentication password

(MPAUT) according to claim 1, but discloses means for generating a random or pseudo random password (MPA), and means for requesting the client site user to provide the authentication password (MPAUT), the authentication password (MPAUT) being derived from the aforesaid random or pseudo random password (MPA).

Claims 1-5, 7, and 9-12 are non-obvious over RATAYCZAK in view of HODGES.

RATAYCZAK discloses a process of securing an access to a data processing server from a client site through at least a first communication network, this server comprising means for handling a protocol of authenticating a client site user. This process allows the secure identification of a user by using two individual connections between a first and a second communications device and an access device, in order to transmit a first code and a second code for checking.

RATAYCZAK illustrates on Figures 3 and 5 two realization modes. Perhaps the most relevant realization mode is illustrated on Figure 5. In this realization mode, the protocol of authenticating a client site user comprises a sequence S51 of receiving and processing identification data ("first code word" column 6 lines 59-64 of RATAYCZAK) from the first communication device C1, and a sequence S52 of transmitting a message ("second code word" column 7 lines 1-5 of RATAYCZAK) from the access device to the second communication device C2 through a second communication network.

In a further step S53, the second code word can be transmitted from the second communication device C2 to the first communication device C1, for example by a read out operation from the first communication device C1 and an input operation at the second communication device C2 (column 7, lines 6-13 of RATAYCZAK). In a further step S54, the second code word is transmitted from the first communication device to access device A and is checked there for correctness (column 7, lines 14-19 of RATAYCZAK).

RATAYCZAK differs from applicants' claim 1 process, in that RATAYCZAK does not disclose wherein the second code word provides the user means for generating an authentication password intended to be transmitted to the server site.

Rather, according to RATAYCZAK, the second code word is just transmitted from the second communication device to the first communication device (column 7, lines 6-9 of RATAYCZAK). In a process according to claim 1 of the application, the user is a person and can realize an intellectual step: a transmitted message provides to him means for generating an authentication password (MPAUT) intended to be transmitted to the server. This intellectual step increases the security level of the process and thus provides an important technical effect.

None of the applied references renders obvious this recited step.

HODGES discloses a method for use in completing a call from a wireless telephone, comprising the steps of receiving a request at a server (or "mobile switching center") from a communication device (or "wireless telephone"), and transmitting a message (or "challenge") from the server to the communication device.

HODGES does not disclose that the challenge provides to the user means for generating an authentication password, but that this challenge provides to the communication device means for generating an authentication password (or "response") intended to be transmitted to the server. This has an important technical effect. A process according to HODGES can not identify the human user of the communication device, but just the communication device.

Consider a process resulting from a combination of RATAYCZAK and HODGES. Such process has the same steps than the process illustrated on RATAYCZAK Figure 5 and previously discussed, and could have the further steps of transmitting a challenge from the server to the first and/or the second communication device, the challenge providing to the first and/or second communication device means for generating an authentication password intended to be transmitted to the server, in order to identify the first and/or the second communication device.

No message provides to the user means for generating an authentication password. As discussed previously, this generating step provides an important technical effect.

Next, consider a cheater who steals the identification data and the mobile phone of a user. In the case of the process according to RATAYCZAK or resulting from a combination of RATAYCZAK and HODGES, the cheater can transmit the identification data to the server (for example by internet), and receive the second code word transmitted to the mobile phone. The cheater can then access to the server. In a process according to the invention, the cheater cannot access to the server, because he does not know how to generate the authentication password.

For these reasons, claim 1 is believed to be novel, non obvious and thus patentable over RATAYCZAK further in view of HODGES.

Claim 2 is dependent upon claim 1. Thus, claim 2 is believed to be patentable over RATAYCZAK further in view of HODGES.

Claim 3 is dependent upon claim 2. Thus, claim 3 is believed to be patentable over RATAYCZAK further in view of HODGES.

Claim 4 is dependent upon claim 3. Thus, claim 4 is believed to be patentable over RATAYCZAK further in view of HODGES.

Claim 5 is dependent upon claim 1. Thus, claim 5 is believed to be patentable over RATAYCZAK further in view of HODGES.

Claim 7 is dependent upon claim 1. Thus, claim 7 is believed to be patentable over RATAYCZAK further in view of HODGES.

Claim 9 is also dependent on claim 1, and claim 12 is directed to an application for utilizing the process of claim 1. Claim 10 discloses the same subject matter as claim 2, and claim 11 discloses the same subject matter as claim 7. Thus, claims 9-12 are believed to be patentable over RATAYCZAK further in view of HODGES.

As to claims 6 and 8 being unpatentable over RATAYCZAK and HODGES, in further view of FIELDER, claim 6 is dependent upon claim 1, and claim 8 is dependent upon claim 7. For these reasons, claims 6 and 8 are believed to be patentable over RATAYCZAK, HODGES, and FIELDER.

Thus, all of the claims are believed non-obvious and patentable.

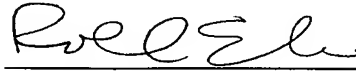
Withdrawal of all of the obviousness rejections is therefore respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any

overpayment to Deposit Account No. 25-0120 for any additional  
fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



---

Roland E. Long, Jr., Reg. No. 41,949  
745 South 23<sup>rd</sup> Street  
Arlington, VA 22202  
Telephone (703) 521-2297  
Telefax (703) 685-0573

REL/lk